

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-150360

(43)Date of publication of application : 23.05.2003

(51)Int.Cl.

G06F 3/12

B41J 5/30

B41J 29/00

B41J 29/38

H04N 1/44

(21)Application number : 2001-351205

(71)Applicant : RICOH CO LTD

(22)Date of filing : 16.11.2001

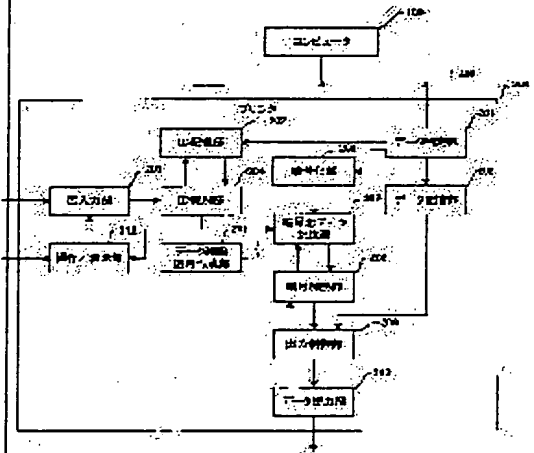
(72)Inventor : NAKAMURA HITOSHI

(54) IMAGE FORMING APPARATUS, SECURITY SYSTEM FOR IMAGE FORMING APPARATUS, SECURITY METHOD FOR IMAGE FORMING APPARATUS AND COMPUTER READABLE STORAGE MEDIUM IN WHICH PROGRAM FOR EXECUTING THE METHOD IS STORED

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an image forming apparatus whose safety can be enhanced by a fact that data can not be illegally taken out by deleting the remaining confidential data at the restart and deleting the confidential data when an unauthorized operation is performed.

SOLUTION: The image forming apparatus is provided with a determination part for determining whether or not data received from a computer is the confidential data, a data storage part for storing the confidential data when the received data is determined as the confidential data by the determination part, an ID storage part for storing and managing an ID of the confidential data, an ID discrimination part for discriminating an inputted ID and the ID stored in the ID storage part by comparing them with each other, a data output part for outputting the confidential data stored in the data storage part when the ID inputted by the ID discrimination part is correct and a data deletion control part for deleting the confidential data stored in the data storage part when a system or the image forming apparatus is restarted.



LEGAL STATUS

[Date of request for examination]

26.08.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

③

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-150360

(P2003-150360A)

(43) 公開日 平成15年5月23日 (2003.5.23)

(51) Int.Cl.⁷

識別記号

F I

テームコード* (参考)

G 0 6 F 3/12

G 0 6 F 3/12

K 2 C 0 6 1

B 4 1 J 5/30

B 4 1 J 5/30

Z 2 C 0 8 7

29/00

29/38

Z 5 B 0 2 1

29/38

H 0 4 N 1/44

5 C 0 7 5

H 0 4 N 1/44

B 4 1 J 29/00

Z

審査請求 未請求 請求項の数10 O L (全 9 頁)

(21) 出願番号

特願2001-351205(P2001-351205)

(71) 出願人 000006747

株式会社リコー

東京都大田区中馬込1丁目3番6号

(22) 出願日

平成13年11月16日 (2001.11.16)

(72) 発明者 中村 仁

東京都大田区中馬込1丁目3番6号 株式

会社リコー内

(74) 代理人 100093920

弁理士 小島 俊郎

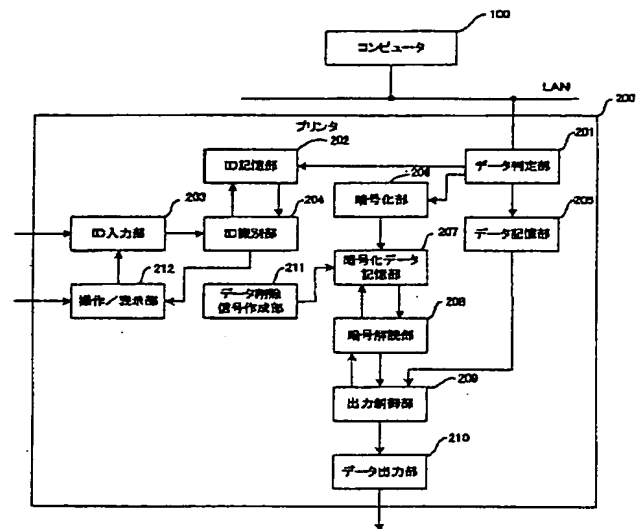
最終頁に続く

(54) 【発明の名称】 画像形成装置、画像形成装置のセキュリティシステム、画像形成装置のセキュリティ方法及び該方法を実行するためのプログラムを格納したコンピュータ読み取り可能な記憶媒体

(57) 【要約】

【解決手段】 本発明は、残った機密データを再起動時に消去することで、また不正操作が行われた場合機密データの消去を行い、データを不正に取り出すことができないことで、安全性を高めることができる画像形成装置を提供することを目的とする。

【解決手段】 本発明の画像形成装置は、コンピュータから受信したデータが機密データである否かを判定する判定部と、判定部によって受信したデータが機密データであるとき当該機密データを記憶するデータ記憶部と、機密データのIDを記憶管理するID記憶部と、入力されたIDとID記憶部に記憶されたIDとを比較して識別するID識別部と、機密データを暗号化する暗号化部と、ID識別部によって入力されたIDが正しい場合はデータ記憶部に記憶された機密データを出力するデータ出力部と、システム又は画像形成装置が再起動された場合データ記憶部に記憶された機密データを消去するデータ消去制御部とを有する。



(2)

【特許請求の範囲】

【請求項1】 ホスト側のコンピュータとネットワークを介して接続され、プリンタ、プリント機能を有する複写機及びFAXなどの画像形成装置において、コンピュータから受信したデータが機密データである否かを判定する判定部と、該判定部によって受信したデータが機密データであるとき当該機密データを記憶するデータ記憶部と、機密データのIDを記憶管理するID記憶部と、入力されたIDと前記ID記憶部に記憶されたIDとを比較して識別するID識別部と、機密データを暗号化する暗号化部と、前記ID識別部によって入力されたIDが正しい場合は前記データ記憶部に記憶された機密データを出力するデータ出力部と、システム又は画像形成装置が再起動された場合前記データ記憶部に記憶された機密データを消去するデータ消去制御部とを有することを特徴とする画像形成装置。

【請求項2】 前記データ消去制御部は、再起動時に、機密データを消去するか否かを選択する請求項1記載の画像形成装置。

【請求項3】 IDの入力が間違っただけの場合に間違っただけの入力回数をカウントする手段と、間違っただけの入力回数が予め設定した所定の回数以上になったとき機密データを消去する手段とを有する請求項1記載の画像形成装置。

【請求項4】 プリンタ、プリント機能を有する複写機及びFAXなどの画像形成装置とホスト側のコンピュータとがネットワークを介して接続され、コンピュータから送信され、画像形成装置から出力される機密データを保護する画像形成装置のセキュリティシステムにおいて、コンピュータは、機密データとしてデータを暗号化する際にキーとなるデータとその他のデータとに分割する分割手段と、キーとなるデータとその他のデータを別々に暗号化して記憶する暗号化記憶手段と、消去された機密データを再度出力する場合キーとなるデータのみを作成して画像形成装置に送信するキー作成部とを有し、画像形成装置は、コンピュータから受信したデータが機密データである否かを判定する判定部と、該判定部によって受信したデータが機密データであるとき当該機密データを記憶するデータ記憶部と、機密データのIDを記憶管理するID記憶部と、入力されたIDと前記ID記憶部に記憶されたIDとを比較して識別するID識別部と、機密データを暗号化する暗号化部と、前記ID識別部によって入力されたIDが正しい場合は前記データ記憶部に記憶された機密データを出力するデータ出力部と、システム又は画像形成装置が再起動された場合キーとなるデータのみを消去するデータ消去制御部とを有することを特徴とする画像形成装置のセキュリティシステム。

【請求項5】 消去された機密データを再度出力する場合前記キー作成部によって作成されたキーによるデータを復元するデータ復元部を有する請求項4記載の画像形成装置のセキュリティシステム。

【請求項6】 画像形成装置は、IDの入力が間違っただけの場合に間違っただけの入力回数をカウントする手段と、間違っただけの入力回数が予め設定した所定の回数以上になったとき機密データを消去する手段とを有する請求項4記載の画像形成装置のセキュリティシステム。

【請求項7】 プリンタ、プリント機能を有する複写機及びFAXなどの画像形成装置とホスト側のコンピュータとがネットワークを介して接続され、コンピュータから送信され、画像形成装置から出力される機密データを保護する画像形成装置のセキュリティ方法において、機密データを保持した状態で、システム又は画像形成装置を再起動する場合、再起動時に、保持された機密データを消去することを特徴とする画像形成装置のセキュリティ方法。

【請求項8】 プリンタ、プリント機能を有する複写機及びFAXなどの画像形成装置とホスト側のコンピュータとがネットワークを介して接続され、コンピュータから送信され、画像形成装置から出力される機密データを保護する画像形成装置のセキュリティ方法において、機密データとしてデータを暗号化する際にキーとその他のデータに分割して各々暗号化し、機密データを保持した状態で、システム又は画像形成装置を再起動する場合、再起動時に、前記キーのみを消去することを特徴とする画像形成装置のセキュリティ方法。

【請求項9】 消去された機密データを再度出力する場合キーを画像形成装置に送信して当該キーによって機密データを復元する請求項8記載の画像形成装置のセキュリティ方法。

【請求項10】 請求項7～9のいずれかに記載の画像形成装置のセキュリティ方法を実行するためのプログラムを格納したコンピュータ読み取り可能な記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は画像形成装置、画像形成装置のセキュリティシステム、画像形成装置のセキュリティ方法及び該方法を実行するためのプログラムを格納したコンピュータ読み出し可能な記憶媒体に関し、詳細にはプリンタ、複写機、ファクシミリ装置及びそれらの各機能を備えた複合機等の画像形成装置により印刷出力される印刷データにおいて、機密指定された印刷データを保護する画像形成装置に関する。

【0002】

【従来の技術】現在、ホスト側のコンピュータとプリンタ等の出力機器側がネットワーク等で接続されたプリンタシステムにおいて、コンピュータ側から出力されたデータが機密データである場合、当該機密データの漏洩を

3

防ぐために、機密データをIDなどにより出力制御を行って保護し、機密データを一旦保持し、IDにより出力の指示を行う方法が採られている。また、機密データを一旦保持するとき、データの暗号化を行いデータの保護を行っている。

【0003】

【発明が解決しようとする課題】しかしながら、上記従来の方法によれば、システムや出力機器の制御に不具合があって再起動を必要とする場合機密データが保持されたままの状態となり、安全性が低くなるという問題点がある。

【0004】本発明はこの問題点を解決するためのものであり、残った機密データを再起動時に消去すること、また不正操作が行われた場合機密データの消去を行い、データを不正に取り出すことができないことで、安全性を高めることができる、画像形成装置、画像形成装置のセキュリティシステム、画像形成装置のセキュリティ方法及び該方法を実行するためのプログラムを格納したコンピュータ読み取り可能な記憶媒体を提供することを目的とする。

【0005】

【課題を解決するための手段】前記問題点を解決するために、ネットワーク環境に接続されたプリンタにおいてシステムや出力機器の不具合により、出力機器の再起動を必要とする場合に機密データとして保持されているデータを再起動時に消去することにより安全性を高める。

【0006】また、再起動時に消去されるデータを一部として、残りのデータは、部分的にも暗号解読不可能な状態として保持し、再度、消去部分に関してのみの少量のデータの再送することで復元可能とすることで、安全性を高める共に処理の高速化を行う。

【0007】更に、不正操作が行われた場合、機密データの消去を行い、データを不正に取り出すことができないようにする。

【0008】

【発明の実施の形態】本発明の画像形成装置は、コンピュータから受信したデータが機密データである否かを判定する判定部と、判定部によって受信したデータが機密データであるとき当該機密データを記憶するデータ記憶部と、機密データのIDを記憶管理するID記憶部と、入力されたIDとID記憶部に記憶されたIDとを比較して識別するID識別部と、機密データを暗号化する暗号化部と、ID識別部によって入力されたIDが正しい場合はデータ記憶部に記憶された機密データを出力するデータ出力部と、システム又は画像形成装置が再起動された場合データ記憶部に記憶された機密データを消去するデータ消去制御部とを有する。

【0009】

【実施例】図1は本発明の一実施例に係る画像形成装置のセキュリティシステムの構成を示すブロック図であ

(3)

4

る。なお、本実施例では画像形成装置をプリンタとして説明するものとする。同図において、セキュリティシステムは、主に、コンピュータ100と、セキュリティ機能を有するプリンタ200とをLANを介して接続した構成を有している。また、プリンタ200は、機密データであるか否かを判定するデータ判定部201と、機密データのためのIDを管理するID記憶部202と、機密データの出力指示のためのIDを入力するID入力部203と、入力されたIDを識別するID識別部204と、機密データ以外のデータを出力するためのデータを記憶するデータ記憶部205と、機密データを暗号化する暗号化部206と、暗号化された機密データを記憶する暗号データ記憶部207と、暗号データを解読する暗号解読部208と、全てのデータの出力制御を行う出力制御部209と、出力データを作像出力するデータ出力部210と、機密データを暗号化データ記憶部207から削除するためのデータ削除信号を作成するデータ削除信号作成部211と、実際にIDを入力したり、入力されたID等や操作ガイダンスを表示する操作/表示部212と、更に図示していないが全体の制御をつかさどるCPUとを含んで構成されている。

【0010】次に、本実施例における機密データを蓄積保持する処理について図1及び機密データ保持動作の動作フローを示す図2に従って説明する。先ず、セキュリティ機能を備えた図1のプリンタ200が図1のコンピュータ100からの出力データを受信すると（ステップS101）、受信したデータが機密データであるか否かを図1のデータ判定部201により判定を行う（ステップS102）。そして、受信したデータが通常のデータである場合、通常のデータ出力のために、一旦データを蓄える図1のデータ記憶部205に出力する。データ記憶部205は、処理状況により、データを記憶保持あるいは、一時的なバッファとして利用される。保持されたデータは、出力制御部209により出力制御される（ステップS102；NO、ステップS103）。一方、出力データが機密データである場合、この出力データは暗号化部206により暗号化処理が行われる（ステップS102；YES、ステップS104）。暗号化されたデータは、暗号データ記憶部207に保持される。暗号化されたデータの保持情報として、記憶場所及びサイズ等を図1のID記憶部202へ出力し、ID記憶部202は、データ受信時に得たID情報と対応付けて、機密データの記憶場所等の情報と共に記憶管理する（ステップS105）。

【0011】次に、本実施例において、出力機器であるプリンタのリセット再起動時の処理について説明すると、このリセット再起動時の処理として、機密データを消去するか否かの情報もID記憶部202により記憶管理する。つまり、図1のID記憶部202での情報管理は、図3に示すように、管理番号、ID、機密データを

50

(4)

5

記憶場所（アドレス等）及びサイズ、システム再起動時に機密データの消去するか否かの情報、などの情報の管理を行う。

【0012】次に、本実施例において、システムの不具合によりシステムの再起動あるいは、プリンタの再起動が行われた場合における機密データの処理方法について図1及び図4に示す動作フローに従って説明する。まず、システム又はプリンタの再起動が行われると、ID記憶部202により管理されている機密データの情報に基づいて機密データがあるかを調べる（ステップS201、S202）。機密データがない場合は、データの消去処理は行われず（ステップS202；NO、ステップS203）。一方、機密データがある場合、図1のID記憶部202で記憶管理している機密データの情報に基づいてシステムリセット時の動作を調べる（ステップS202；YES、ステップS204）。システムリセット時の動作として、機密データの消去を行わない場合、データの消去処理は行われず、次の機密データの処理を行う（ステップS204；NO、ステップS205）。一方、機密データの消去を行う場合、ID記憶部202で記憶管理している機密データの情報に基づいてそのデータの記憶場所（アドレス）を調べ、図1の暗号データ記憶部207に記憶されている機密データの消去をデータ削除信号作成部211の制御により消去を行う（ステップS204；YES、ステップS206）。また、ID記憶部202の情報も削除する（ステップS207）。この処理を機密データ全てに関して、繰り返すことにより、リセット再起動時に、機密データの消去が可能である。

【0013】図5は本実施例における機密データとkeyデータの蓄積の処理フローを示すフローチャートである。同図において、まず機密データの出力命令が図1のコンピュータ100より出力されると、コンピュータ100は、機密データをkeyとその他のデータに分割する（ステップS301、S302）。そして、プリンタ200へ分割したkeyデータとその他のデータを送信する（ステップS303）。プリンタ200は、コンピュータ100からのデータを受信し、受信したデータが機密データであるか判断する（ステップS304、ステップS305）。そして、機密データでない場合は、通常データとして出力を行う（ステップS305；NO、ステップS306）。一方、機密データである場合は、keyデータとその他のデータをそれぞれ暗号化される（ステップS305；YES、ステップS307）。そして、暗号化されたkeyデータとその他のデータを蓄積する（ステップS308）。なお、機密データの情報管理として、図6に示すように、データの登録番号、ID番号、機密データのkey以外の暗号化データの記憶場所（アドレス）、データのサイズ、keyデータの記憶場所（アドレス）、起動時にデータを消去す

6

る否かの判断の情報を管理記憶する。

【0014】次に、本実施例において、システムの再起動あるいは、プリンタの再起動が行われた場合における機密データのkeyデータの消去及び消去された状態から機密データを復元する処理について図1及び図7に示す動作フローに従って説明する。まず、システム又はプリンタが再起動されると、図1のID記憶部202にて記憶管理されている情報より、機密データの有無を調べる（ステップS401、S402）。機密データがない場合、機密データの消去処理は終了となる（ステップS402；NO、ステップS403）。一方、機密データがある場合、起動時のデータ消去を行うか否かの情報を調べる（ステップS402；YES、ステップS404）。そして、起動時のデータ消去を行わない場合、次のデータの処理を行う（ステップS404；NO、ステップS405）。一方、起動時のデータ消去を行う場合、keyデータ部分のみ消去する（ステップS404；YES、ステップS406）。また、ID記憶部情報のkey情報を削除する（ステップS407）。なお、key情報の削除は、図7に示すように、管理番号0003のkeyデータのアドレスを“eeeeeee”のように特定の値とする。この特定の値により、keyが削除されたものとする。上記一連の処理を全機密データに対して繰り返す。

【0015】次に、本実施例におけるkeyが削除されたデータを再度出力する処理について当該処理フローを示す図8に従って説明する。まず、再起動されたシステムにおいてkeyが消去されたデータを出力するために、消去された機密データの再送の指示する（ステップS501）。コンピュータ100側は、データからkeyとなるデータを作成する（ステップS502）。ここで、出力機器であるプリンタ200中のkeyデータと、コンピュータ100が作成するkeyデータと一致するように指示して作成する。なお、keyデータの作り方は、指示することにより、作成データを変更可能とする。その後、出力機器であるプリンタ200へデータを送信する（ステップS503）。出力機器であるプリンタ200側は、受信したデータが機密データであるか判断を行う（ステップS504）。機密データでない場合は、通常出力処理を行う（ステップS504；NO、ステップS505）。一方、機密データである場合は、受信したデータがkeyによるデータの復元であるか判断する（ステップS504；YES、ステップS506）。keyによる復元でない場合、機密データとしてデータの蓄積を行う（ステップS506；NO、ステップS507）。一方、keyによる復元である場合、keyデータの暗号化を行い、データを蓄積する。また、IDデータ記憶部の情報を該当する機密データの情報の復元して記憶する（ステップS506；YES、ステップS508、S509）。以上の一連の処理で、

7

keyに関するデータ及び情報を復元し、機密データの出力が可能な状態となる。

【0016】次に、本実施例における出力機器であるプリンタから機密データの出力要求がIDの入力が不正である場合にデータの保護のため機密データを削除する処理について当該処理フローを示す図9に従って説明する。なお、一例として、不正に出力指示した回数によりデータを消去する処理手順を説明する。

【0017】先ず、出力機器である図1のプリンタ200の操作/表示部212より機密データの出力指示がされると、IDの入力を促すメッセージを表示し、IDの入力待ちとなる(ステップS601、S602)。そして、IDが入力されると、IDに該当する機密データが保持されているか否か判断する(ステップS603、S604)。該当するデータが存在する場合は、機密データを読み出し、暗号解読処理を行って、データのプリントアウトを行う(ステップS604; YES、ステップS605~S607)。一方、該当するデータが存在しない場合、不正に機密データを出力させようとしているものと判断する。不正と判断した場合をカウントする(ステップS604; NO、ステップS608)。そして、不正と判断した回数が設定した所定値以上でない場合、指示待ちの状態に戻る(ステップS609; NO)。一方、不正と判断した回数が設定した所定値以上である場合、機密データの消去を行う(ステップS609; YES、ステップS610)。なお、機密データの消去方法は、前述のように行う。

【0018】次に、図10は本発明のシステム構成を示すブロック図である。つまり、同図は上記実施例における画像形成装置のセキュリティ方法によるソフトウェアを実行するマイクロプロセッサ等から構築されるハードウェアを示すものである。同図において、画像形成装置のセキュリティシステムはインターフェース(以下I/Fと略す)101、CPU102、ROM103、RAM104、表示装置105、ハードディスク106、キーボード107及びCD-ROMドライブ108を含んで構成されている。また、汎用の処理装置を用意し、CD-ROM109などの読取可能な記憶媒体には、本発明の画像形成装置のセキュリティ方法を実行するプログラムが記憶されている。更に、I/F101を介して外部装置から制御信号が入力され、キーボード107によって操作者による指令又は自動的に本発明のプログラムが起動される。そして、CPU102は当該プログラムに従って上述の画像形成装置のセキュリティ方法に伴う制御処理を施し、その処理結果をRAM104やハードディスク106等の記憶装置に格納し、必要により表示装置105などに出力する。以上のように、本発明の画像形成装置のセキュリティ方法を実行するプログラムが記憶した媒体を用いることにより、既存のシステムを変えることなく、画像形成装置のセキュリティシステムを

(5)

8

汎用的に構築することができる。

【0019】なお、本発明は上記実施例に限定されるものではなく、特許請求の範囲内の記載であれば多種の変形や置換可能であることは言うまでもない。

【0020】

【発明の効果】以上説明したように、本発明の画像形成装置は、コンピュータから受信したデータが機密データである否かを判定する判定部と、判定部によって受信したデータが機密データであるとき当該機密データを記憶するデータ記憶部と、機密データのIDを記憶管理するID記憶部と、入力されたIDとID記憶部に記憶されたIDとを比較して識別するID識別部と、機密データを暗号化する暗号化部と、ID識別部によって入力されたIDが正しい場合はデータ記憶部に記憶された機密データを出力するデータ出力部と、システム又は画像形成装置が再起動された場合データ記憶部に記憶された機密データを消去するデータ消去制御部とを有することに特徴がある。よって、ネットワーク環境に接続されたプリンタ等の画像形成装置においてシステムや画像形成装置の不具合により、システム又は画像形成装置の再起動を必要とする場合に機密データとして保持されているデータを再起動時に消去することより安全性を高めることができる。

【0021】また、データ消去制御部は、再起動時に、機密データを消去するか否かを選択することにより、画像形成装置側で機密データの出力を管理することができる。

【0022】更に、IDの入力が間違っただけの場合に間違っただけの入力回数をカウントする手段と、間違っただけの入力回数が予め設定した所定の回数以上になったとき機密データを消去する手段とを有することにより、不正操作が行われた場合、機密データの消去を行い、データを不正に取り出すことができないようにすることができる。

【0023】また、別の発明としての画像形成装置のセキュリティシステムによれば、コンピュータは、機密データとしてデータを暗号化する際にキーとなるデータとその他のデータとに分割する分割手段と、キーとなるデータとその他のデータを別々に暗号化して記憶する暗号化記憶手段と、消去された機密データを再度出力する場合キーとなるデータのみを作成して画像形成装置に送信するキー作成部とを有し、画像形成装置は、コンピュータから受信したデータが機密データである否かを判定する判定部と、判定部によって受信したデータが機密データであるとき当該機密データを記憶するデータ記憶部と、機密データのIDを記憶管理するID記憶部と、入力されたIDとID記憶部に記憶されたIDとを比較して識別するID識別部と、機密データを暗号化する暗号化部と、ID識別部によって入力されたIDが正しい場合はデータ記憶部に記憶された機密データを出力するデータ出力部と、システム又は画像形成装置が再起動され

50

(6)

9

た場合キーとなるデータのみを消去するデータ消去制御部とを有する。よって、このような構成を有するセキュリティシステムによれば、ネットワーク環境に接続されたプリンタ等の画像形成装置においてシステムや画像形成装置の不具合により、システム又は画像形成装置の再起動を必要とする場合に機密データとして保持されているデータを再起動時に消去することより安全性を高めることができる。

【0024】また、消去された機密データを再度出力する場合キー作成部によって作成されたキーによるデータを復元するデータ復元部を有することにより、再起動時に消去されるデータを一部として、残りのデータは、部分的にも暗号解読不可能な状態として保持し、再度、消去部分に関してのみの少量のデータの再送することで復元可能とすることで、安全性を高める共に処理の高速化を図ることができる。

【0025】更に、セキュリティシステムにおける画像形成装置は、IDの入力が間違っした場合に間違っ入力回数をカウントする手段と、間違っ入力回数が予め設定した所定の回数以上になったとき機密データを消去する手段とを有することにより、不正操作が行われた場合、機密データの消去を行い、データを不正に取り出すことができないようにすることができる。

【0026】また、別の発明として画像形成装置のセキュリティ方法によれば、機密データを保持した状態で、システム又は画像形成装置を再起動する場合、再起動時に、保持された機密データを消去する。よって、機密データとして保持されているデータを再起動時に消去することより安全性を高めることができる。

【0027】更に、機密データとしてデータを暗号化する際にキーとその他のデータに分割して各々暗号化し、機密データを保持した状態で、システム又は画像形成装置を再起動する場合、再起動時に、キーのみを消去することにより、機密データとして保持されているデータを再起動時に消去することより安全性を高めることができる。

【0028】また、消去された機密データを再度出力する場合キーを画像形成装置に送信して当該キーによって機密データを復元することにより、安全性を高める共に処理の高速化を図ることができる。

【図3】

管理番号	ID	データ記憶 アドレス	サイズ	起動時データ 消去
0001	abc12348	1000000	XXXX	1
0002	abc12345	1002000	XXXX	0
0003		1004000		

10

【0029】更に、上記記載の画像形成装置のセキュリティ方法を実行するためのプログラムを格納したコンピュータ読み取り可能な記憶媒体に特徴がある。よって、本発明の画像形成装置のセキュリティ方法を実行するプログラムが記憶した媒体を用いることにより、既存のシステムを変えることなく、画像形成装置のセキュリティシステムを構築する装置を汎用的に使用することができる。

【図面の簡単な説明】

10 【図1】本発明の一実施例に係る画像形成装置のセキュリティシステムの構成を示すブロック図である。

【図2】本実施例における機密データ保持動作を示すフローチャートである。

【図3】図1のID記憶部での情報管理内容を示す図である。

【図4】再起動時の機密データの処理を示すフローチャートである。

【図5】本実施例における機密データとkeyデータの蓄積の処理フローを示すフローチャートである。

20 【図6】図1のID記憶部での別の情報管理内容を示す図である。

【図7】本実施例における再起動時の機密データのkeyデータの消去及び消去された状態から機密データを復元する処理を示すフローチャートである。

【図8】本実施例におけるkeyが削除されたデータを再度出力する処理を示すフローチャートである。

30 【図9】本実施例における出力機器であるプリンタから機密データの出力要求がIDの入力が不正である場合にデータの保護のため機密データを削除する処理を示すフローチャートである。

【図10】本発明のシステム構成を示すブロック図である。

【符号の説明】

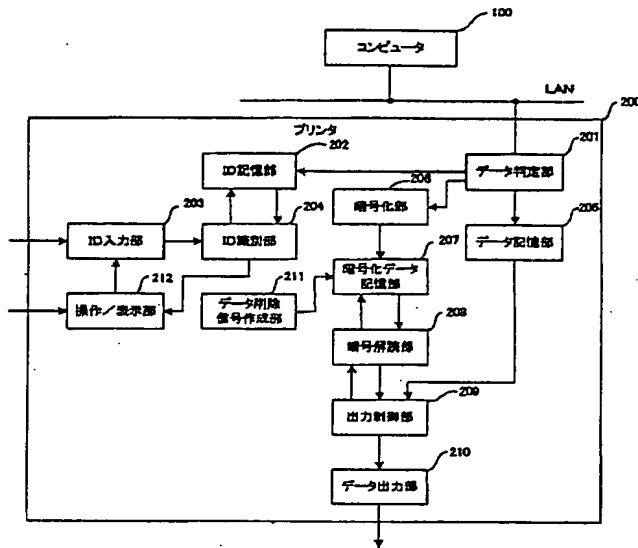
100；コンピュータ、200；プリンタ、201；データ判定部、202；ID記憶部、203；ID入力部、204；ID識別部、205；データ記憶部、206；暗号化部、207；暗号化データ記憶部、208；暗号解読部、209；出力制御部、210；データ出力部、211；データ削除信号作成部、212；操作／表示部。

【図7】

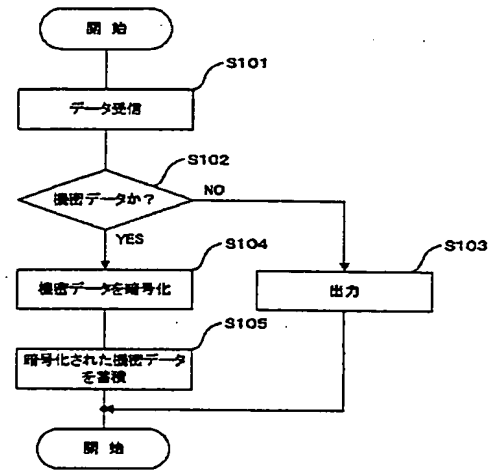
管理番号	ID	データ記憶 アドレス	Keyデータ アドレス	サイズ	起動時データ 消去
0001	abc12348	1000000	a000000	XXXX	1
0002	abc12345	1002000	a0001000	XXXX	0
0003	abc11111	1004000	aaaaaaa		

(7)

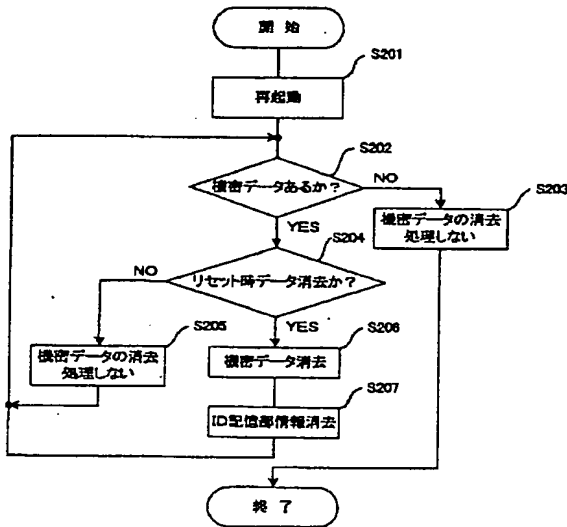
【図1】



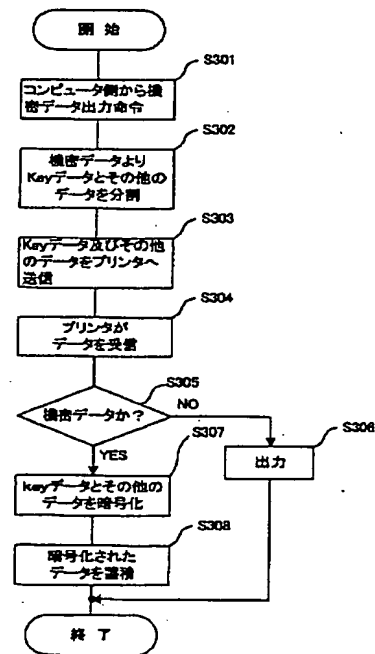
【図2】



【図4】

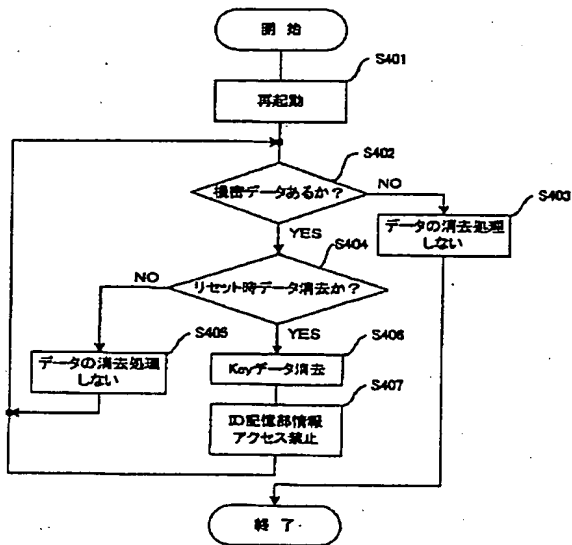


【図5】

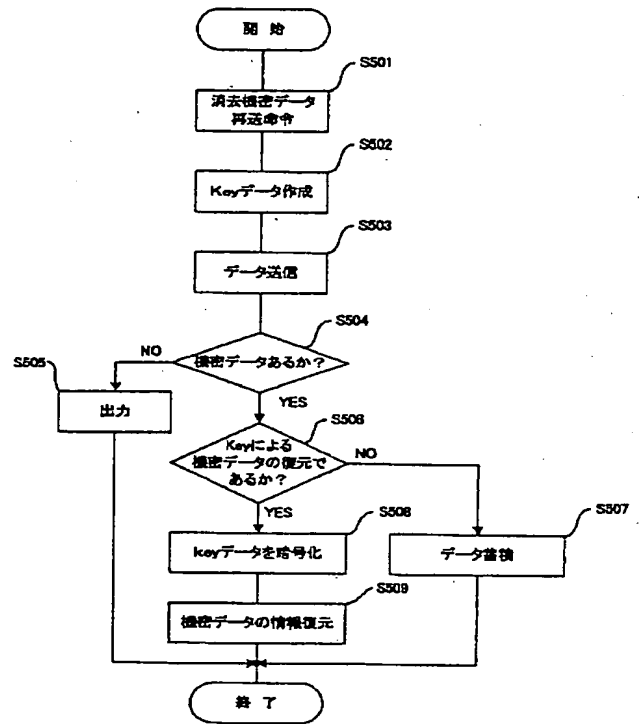


(8)

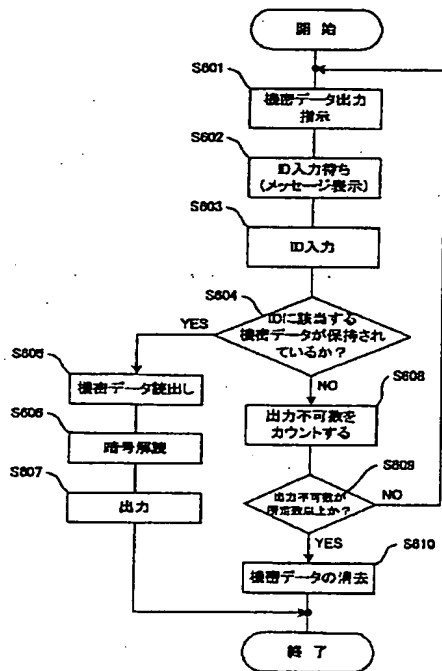
【図6】



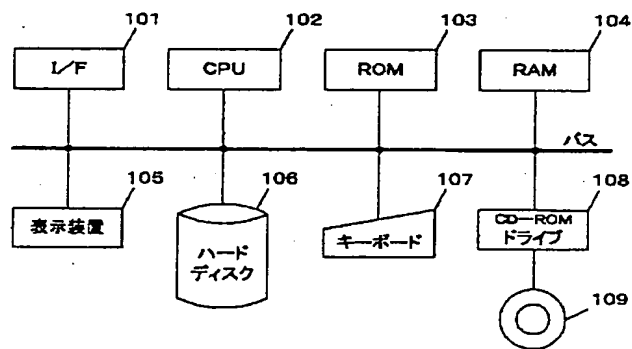
【図8】



【図9】



【図10】



(9)

フロントページの続き

F ターム(参考) 2C061 AP01 AP03 AP04 AP07 BB17
CL08 CL10 HJ06 HK23 HN23
2C087 AA03 AA09 AB05 BA14 BC04
BC06 DA13
5B021 AA02 BB01 BB04 BB09 CC05
5C075 AA90 AB90 EE02 EE03 EE90
FF90